

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1 1. (currently amended) A method for managing a network, comprising the steps of:
2 detecting occurrence of a network event, said network event having associated
3 with it a network condition comprising at least one of an unplanned macro-event and a
4 planned macro-event related to at least one of a network element and a communication
5 link of said network;

6 classifying said network event as being at least one of a network element failure, a
7 communications link failure, and a security breach; and

8 identifying said network event as a network degradation event in response to at
9 least one network event exceeding a network degradation threshold, wherein said
10 network degradation event is defined as at least one of a brink of failure (BOF) event and
11 a breach of security (BOS) event, wherein if said network degradation event is defined as
12 a BOF event a determination is made as to whether said BOF event also causes a BOS
13 event, wherein if said network degradation event is defined as a BOS event a
14 determination is made as to whether said BOS event also causes a BOF event.

1 2. (original) The method of claim 1, further comprising the step of:
2 sending an alert to normalize said network degradation event.

1 3. (original) The method of claim 1, wherein said network event is associated with at
2 least one of a network management system, a security management system, and a system
3 timer.

1 4. (currently amended) The method of claim 1, wherein said step of identifying
2 comprises the step of:

3 defining said network degradation event as a brink of failure (BOF) event in an
4 instance where said network event is at least one of a type determined to cause a failure
5 of at least one network element within a predetermined time interval, a type determined
6 to affect at least one ~~of~~^a critically defined network functionality, and a type determined
7 to affect a number of end users exceeding a predetermined threshold level.

1 5. (currently amended) The method of claim [[4]] 1, wherein said step of identifying
2 said network degradation event comprises the step of:

3 assessing at least one of failure rates, mean-time-between-failures (MTBF), mean-
4 time-to-repair (MTTR), and spare parts availability for at least one of network elements
5 and communication links associated with said network event.

1 6. (original) The method of claim 1, wherein in response to the step of classifying
2 said network event, said method further comprises the steps of:

3 updating an existing conditions database with indicia of said network event;
4 determining a latest network topology associated with said network event; and
5 updating a network topology database with said latest network topology.

1 7. (original) The method of claim 4, wherein said step of identifying further
2 comprises the step of:

3 defining said network degradation event as a breach-of-security (BOS) event in an
4 instance where said network event exploits a security vulnerability resulting in at least
5 one of an unauthorized access, an unauthorized modification or compromise, a denial of
6 access to information, a denial of access to network monitoring capability, and a denial of
7 access to network control capability.

1 8. (currently amended) The method of claim [[7]] 4, wherein said step of defining
2 said network degradation event as a brink-of-failure (BOF) event further comprises the
3 step of:

4 correlating network events stored in said an existing conditions database with
5 information stored in said a network topology database and events stored in a scheduled
6 events database.

1 9. (currently amended) The method of claim [[8]] 7, further comprising the steps of:
2 ~~determining whether said BOF event also causes a BOS event;~~
3 ~~determining whether said BOS event also causes a BOF;~~ and
4 reporting at least one of said BOF event and BOS event.

1 10. (original) The method of claim 9 further comprising the steps of:
2 categorizing said BOF event;
3 determining at least one corrective action procedure associated with said BOF
4 event; and
5 reporting at least one of a network element and a communications link associated
6 with said BOF event, and said at least one corrective action procedure.

1 11. (original) The method of claim 10, wherein said step of determining at least one
2 corrective action procedure comprises the step of assessing a BOF database comprising
3 historical information associated with global network reliability practices.

1 12. (currently amended) The method of claim 9, wherein in an instance where said
2 network degradation event is associated with a ~~breach-of-security~~ BOS event, said
3 method further comprises the steps of:
4 categorizing said ~~breach-of-security~~ BOS event;
5 determining at least one corrective action procedure associated with said ~~breach~~
6 ~~of security~~ BOS event; and
7 displaying at least one of a network element and a communications link
8 associated with said ~~breach-of-security~~ BOS event, and said at least one corrective action
9 procedure.

1 13. (original) The method of claim 12, wherein said step of determining at least one
2 corrective action procedure comprises the step of assessing a Security Vulnerabilities and
3 Procedures database comprising at least one of historical information of said network and
4 associated global security vulnerabilities and procedures.

1 14. (original) The method of claim 1, wherein said step of identifying a network event
2 comprises the step of identifying events associated with at least one of end-user data
3 traffic, in-band control traffic, out-of-band control traffic, in-band network management
4 traffic, and out-of-band network management traffic.

1 15. (original) The method of claim 9 further comprising the steps of:
2 initiating a new network event upon resolving said network degradation event;
3 removing said network degradation event from said existing conditions database;
4 and
5 reporting said network degradation event as a resolved event.

1 16. (currently amended) The method of claim 15, wherein resolving said network
2 degradation event further comprises ~~the step of~~ at least one of:
3 resolving said BOF event, such that the BOF event and a BOS condition are
4 cleared; and
5 resolving said BOS event, such that the BOS event and a BOF condition are
6 cleared.

1 17. (currently amended) A method for managing a network, comprising the steps of:
2 detecting occurrence of a network event, said network event having associated
3 with it a network condition comprising at least one of an unplanned macro-event and a
4 planned macro-event related to at least one of a network element and a communication
5 link of said network;
6 classifying said network event as being at least one of a network element failure, a
7 communications link failure, and a security breach;

8 identifying said network event as a network degradation event in response to at
9 least one network event exceeding a network degradation threshold by defining said
10 network degradation event as a brink of failure (BOF) event in an instance where said
11 network event is at least one of a type determined to cause a failure of at least one
12 network element within a predetermined time interval, a type determined to affect at least
13 one ~~of~~ a critically defined network functionality, and a type determined to affect a
14 number of end users exceeding a predetermined threshold level;
15 determining whether said BOF event also causes a BOS event; and
16 sending an alert to normalize said network degradation event.

1 18. (original) The method of claim 17, wherein said step of identifying further
2 comprises the step of:

3 defining said network degradation event as a breach-of-security (BOS) event in an
4 instance where said network event exploits a security vulnerability resulting in at least
5 one of an unauthorized access, an unauthorized modification or compromise, a denial of
6 access to information, a denial of access to network monitoring capability, and a denial of
7 access to network control capability.

1 19. (original) The method of claim 18, wherein in response to the step of classifying
2 said network event, said method further comprises the steps of:

3 updating an existing conditions database with indicia of said network event;
4 determining a latest network topology associated with said network event; and
5 updating a network topology database with said latest network topology.

1 20. (currently amended) The method of claim [[19]] 18, further comprising the steps
2 of:

3 determining whether said BOF event also causes a BOS event;
4 determining whether said BOS event also causes a BOF event; and
5 reporting at least one of said BOF event and BOS event.

1 21. (original) The method of claim 20 further comprising the steps of:

2 categorizing said BOF event;
3 determining at least one corrective action procedure associated with said BOF
4 event; and
5 reporting at least one of a network element and a communications link associated
6 with said BOF event, and said at least one corrective action procedure.

1 22. (currently amended) The method of claim 20, wherein in an instance where said
2 network degradation event is associated with a ~~breach-of-security~~ BOS event, said
3 method further comprises the steps of:

4 categorizing said ~~breach-of-security~~ BOS event;
5 determining at least one corrective action procedure associated with said ~~breach~~
6 ~~of-security~~ BOS event; and
7 displaying at least one of a network element and a communications link
8 associated with said ~~breach-of-security~~ BOS event, and said at least one corrective action
9 procedure.

1 23. (currently amended) The method of claim [[19]] 20, further comprising the steps
2 of:
3 initiating a new network event upon resolving said network degradation event;
4 removing said network degradation event from said existing conditions database;
5 and
6 reporting said network degradation event as a resolved event.

1 24. (currently amended) Apparatus for managing a network, comprising:
2 means for detecting occurrence of a network event, said network event having
3 associated with it a network condition comprising at least one of an unplanned macro-
4 event and a planned macro-event related to at least one of a network element and a
5 communication link of said network;
6 means for classifying said network event as being at least one of a network
7 element failure, a communications link failure, and a security breach; and

8 means for identifying said network event as a network degradation event in
9 response to at least one network event exceeding a network degradation threshold,
10 wherein said network degradation event is defined as at least one of a brink of failure
11 (BOF) event and a breach of security (BOS) event;

12 means for determining whether a network degradation event defined as a BOF
13 event also causes a BOS event; and

14 means for determining whether a network degradation event defined as a BOS
15 event also causes a BOF event.

1 25. (original) The apparatus of claim 24, further comprising:

2 means for sending an alert to normalize said network degradation event.

1 26. (currently amended) The apparatus of claim 24, wherein said means for
2 identifying comprises:

3 means for defining said network degradation event as a brink of failure (BOF)
4 event in an instance where said network event is at least one of a type determined to
5 cause a failure of at least one network element within a predetermined time interval, a
6 type determined to affect at least one of a critically defined network functionality, and a
7 type determined to affect a number of end users exceeding a predetermined threshold
8 level.

1 27. (original) The apparatus of claim 26, wherein said means for identifying further
2 comprises:

3 means for defining said network degradation event as a breach-of-security (BOS)
4 event in an instance where said network event exploits a security vulnerability resulting
5 in at least one of an unauthorized access, an unauthorized modification or compromise, a
6 denial of access to information, a denial of access to network monitoring capability, and a
7 denial of access to network control capability.

1 28. (currently amended) The apparatus of claim 24, wherein said means for
2 classifying further comprises:

3 means for updating an existing conditions database with indicia of said network
4 event;
5 means for determining a latest network topology associated with said network
6 event; and
7 means for updating a network topology database with said latest network
8 topology.

1 29. (currently amended) The apparatus of claim [[26]] 27, further comprising:
2 ~~means for determining whether said BOF event also causes a BOS event;~~
3 ~~means for determining whether said BOS event also causes a BOF;~~ and
4 means for reporting at least one of said BOF event and BOS event.

1 30. (original) The apparatus of claim 29 further comprising:
2 means for categorizing said BOF event;
3 means for determining at least one corrective action procedure associated with
4 said BOF event; and
5 means for reporting at least one of a network element and a communications link
6 associated with said BOF event, and said at least one corrective action procedure.

1 31. (currently amended) The apparatus of claim 29, wherein ~~in an instance where said~~
2 ~~network degradation event is associated with a breach-of-security event,~~ said apparatus
3 further comprises:
4 means for categorizing, in an instance where said network degradation event is
5 associated with a BOS event, said breach-of-security said BOS event;
6 means for determining at least one corrective action procedure associated with
7 ~~said breach-of-security~~ BOS event; and
8 means for displaying at least one of a network element and a communications link
9 associated with said ~~breach-of-security~~ BOS event, and said at least one corrective action
10 procedure.

1 32. (original) The apparatus of claim 29 further comprising:

2 means for initiating a new network event upon resolving said network degradation
3 event;
4 means for removing said network degradation event from said existing conditions
5 database; and
6 means for reporting said network degradation event as a resolved event.

1 33. (original) The apparatus of claim 32, wherein resolving said network degradation
2 event further comprises at least one of:
3 means for resolving said BOF event, such that the BOF event and a BOS
4 condition are cleared; and
5 means for resolving said BOS event, such that the BOS event and a BOF
6 condition are cleared.

1 34. (currently amended) A network management system for characterizing at least
2 one network degradation event in a communications network, comprising:
3 a processing unit having access to at least one storage device;
4 at least a portion of said at least one storage device having a program product
5 configured to:
6 detect occurrence of a network event, said network event having associated with it
7 a network condition comprising at least one of an unplanned macro-event and a planned
8 macro-event related to at least one of a network element and a communication link of
9 said network;
10 classify said network event as being at least one of a network element failure, a
11 communications link failure, and a security breach; and
12 identify said network event as a network degradation event in response to at least
13 one network event exceeding a network degradation threshold, wherein said network
14 degradation event is defined as at least one of a brink of failure (BOF) event and a breach
15 of security (BOS) event, wherein if said network degradation event is defined as a BOF
16 event a determination is made as to whether said BOF event also causes a BOS event,
17 wherein if said network degradation event is defined as a BOS event a determination is
18 made as to whether said BOS event also causes a BOF event.